

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11355265 A**

(43) Date of publication of application: **24 . 12 . 99**

(51) Int. Cl.

H04L 9/14
G06F 13/00
G06F 13/00
H04H 1/00
H04L 9/32
H04L 29/08
H04N 7/167
// G06F 13/38
H04L 12/28

(21) Application number: **10162667**

(22) Date of filing: **10 . 06 . 98**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

(72) Inventor: **NISHIMURA TAKUYA**
IIZUKA HIROYUKI
YAMADA MASAZUMI
GOTO SHOICHI
TAKECHI HIDEAKI

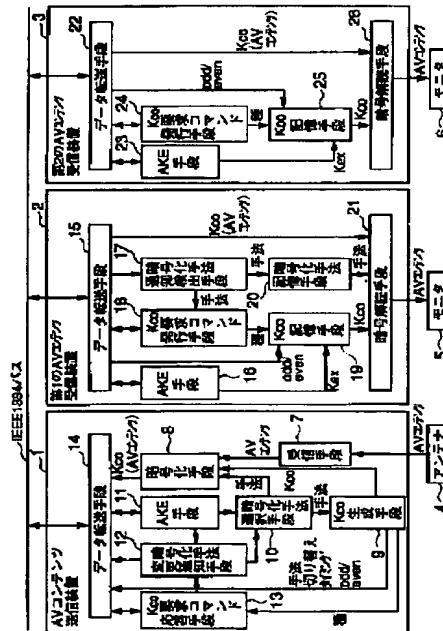
(54) **METHOD FOR AV CONTENTS TRANSMISSION AND AV CONTENTS RECEPTION, DEVICE FOR AV CONTENTS TRANSMISSION AND AV CONTENTS RECEPTION AND MEDIUM**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an AV contents transmission method that an AV contents receiver, which cannot use a first enciphering method when an AV contents transmitter is receiving the AV contents enciphered by the first enciphering method, can decode its AV contents.

SOLUTION: If there is a authentication demand from a second contents receiver which cannot use an extended enciphering method while an AV contents transmitter 1 is transmitting AV contents enciphered by the extended enciphering method by using an IEEE 1394 bus, then after the authentication is successful, the AV contents transmitter 1 enciphers the AV contents by a basic enciphering method, which a second AV contents receiver 3 making the authentication demand can use, and transmits them.

COPYRIGHT: (C)1999,JPO



(51)Int.Cl.⁹

識別記号

F I

H 0 4 L 9/14

H 0 4 L 9/00

6 4 1

G 0 6 F 13/00

3 5 1

G 0 6 F 13/00

3 5 1 A

3 5 7

3 5 7 A

H 0 4 H 1/00

H 0 4 H 1/00

F

H 0 4 L 9/32

G 0 6 F 13/38

3 5 0

審査請求 未請求 請求項の数20 O L (全 15 頁) 最終頁に続く

(21)出願番号

特願平10-162667

(22)出願日

平成10年(1998) 6 月10日

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 西村 拓也

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 飯塚 裕之

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 山田 正純

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74)代理人 弁理士 松田 正道

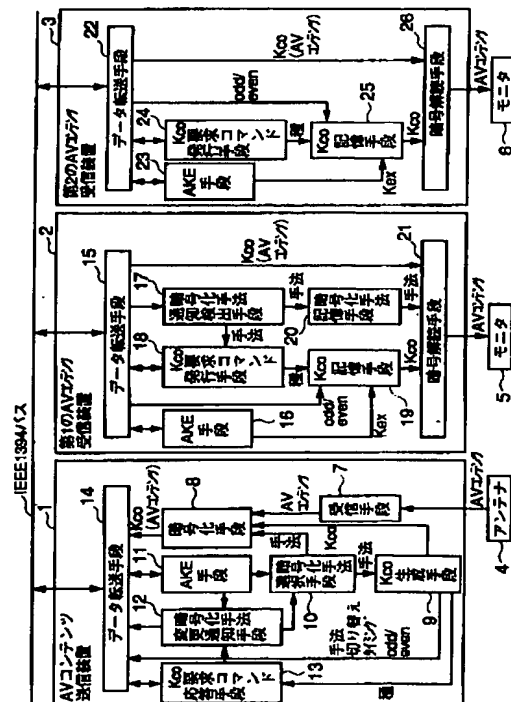
最終頁に続く

(54)【発明の名称】 AVコンテンツ送信方法、AVコンテンツ受信方法、AVコンテンツ送信装置、AVコンテンツ受信装置および媒体

(57)【要約】

【課題】 AVコンテンツ送信装置が拡張暗号化手法で暗号化したAVコンテンツを送信しているときに、その拡張暗号化手法を使用することができないAVコンテンツ受信装置はそのAVコンテンツを解読することができない。

【解決手段】 AVコンテンツ送信装置1がIEEE1394バスを利用して拡張暗号化手法で暗号化したAVコンテンツを送信しているときに、その拡張暗号化手法を使用することができない第2のAVコンテンツ受信装置3から認証要求があると、その認証が成功した後、AVコンテンツ送信装置1は、その認証要求をした第2のAVコンテンツ受信装置3が使用することができる基本暗号化手法でAVコンテンツを暗号化して送信する。



【特許請求の範囲】

【請求項 1】ＡＶコンテンツ送信装置が伝送路を利用して第 1 の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、

その第 1 の暗号化手法を使用することができないＡＶコンテンツ受信装置から認証要求があると、

その認証要求をしたＡＶコンテンツ受信装置が使用することができる第 2 の暗号化手法で前記ＡＶコンテンツを暗号化して送信することを特徴とするＡＶコンテンツ送信方法。

【請求項 2】前記認証要求があったさい、既にそれまでの前記第 1 の暗号化手法で暗号化されたＡＶコンテンツを受信し解読していた、前記認証要求をしたＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置がある場合、

その別のＡＶコンテンツ受信装置に、暗号化手法が前記第 2 の暗号化手法に切り替わることを通知することを特徴とする請求項 1 記載のＡＶコンテンツ送信方法。

【請求項 3】前記暗号化手法の切り替えを、所定のコマンドを用いて、または前記ＡＶコンテンツのなかに付加して通知することを特徴とする請求項 2 記載のＡＶコンテンツ送信方法。

【請求項 4】前記切り替えた後の前記第 2 の暗号化手法がどのような暗号化手法であるのかという情報を、所定のコマンドを用いて、または前記ＡＶコンテンツのなかに付加して通知することを特徴とする請求項 3 記載のＡＶコンテンツ送信方法。

【請求項 5】前記切り替えた後の前記第 2 の暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を、所定のコマンドを用いて、または前記ＡＶコンテンツのなかに付加して通知することを特徴とする請求項 3 記載のＡＶコンテンツ送信方法。

【請求項 6】前記暗号化手法の切り替えのタイミングを、前記認証要求がある前に使用していた前記第 1 の暗号化手法での暗号化鍵の更新のタイミングとすることを特徴とする請求項 1 記載のＡＶコンテンツ送信方法。

【請求項 7】少なくとも前記別のＡＶコンテンツ受信装置に、前記暗号化手法が前記第 2 の暗号化手法に切り替わることを通知するとともに、その暗号化手法の切り替えのタイミングの情報を送信することを特徴とする請求項 2 記載のＡＶコンテンツ送信方法。

【請求項 8】前記ＡＶコンテンツ送信装置が前記認証要求をしたＡＶコンテンツ受信装置を記憶し、

そのＡＶコンテンツ受信装置から、前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなった場合、

前記暗号化手法を前記第 2 の暗号化手法から前記第 1 の暗号化手法に切り替えることを特徴とする請求項 1 記載のＡＶコンテンツ送信方法。

【請求項 9】前記ＡＶコンテンツ送信装置が、前記認証要求をしたＡＶコンテンツ受信装置と前記そのＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドを送信してくるＡＶコンテンツ受信装置が、全て前記第 1 の暗号化手法を使用することができるＡＶコンテンツ受信装置である場合、

前記暗号化手法を前記第 2 の暗号化手法から前記第 1 の暗号化手法に切り替えることを特徴とする請求項 1 記載のＡＶコンテンツ送信方法。

【請求項 1 0】請求項 1 から 9 のいずれかに記載のＡＶコンテンツ送信方法の各ステップの全部または一部を実現するためのプログラムを格納したことを特徴とする媒体。

【請求項 1 1】請求項 1 から 9 のいずれかに記載のＡＶコンテンツ送信方法によって送信されてくるＡＶコンテンツを受信し、

そのＡＶコンテンツが暗号化されたさいに使用された暗号化手法に基づくとともに、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたＡＶコンテンツを解読することを特徴とするＡＶコンテンツ受信方法。

【請求項 1 2】請求項 1 から 9 のいずれかに記載のＡＶコンテンツ送信方法によって送信されてくるＡＶコンテンツとともに、またはそのＡＶコンテンツのなかに、前記暗号化手法の切り替えに関する情報があって、

その情報に、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種との一方または両方が含まれていない場合、

前記ＡＶコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記暗号化手法の切り替えに関する情報に含まれていないものを送信するように要求することを特徴とする請求項 1 1 記載のＡＶコンテンツ受信方法。

【請求項 1 3】請求項 1 1 または 1 2 記載のＡＶコンテンツ受信方法の各ステップの全部または一部を実現するためのプログラムを格納したことを特徴とする媒体。

【請求項 1 4】送信しようとするＡＶコンテンツを暗号化するさいの暗号化手法を選択する暗号化手法選択手段と、

その暗号化手法選択手段によって選択された暗号化手法に対応した、ＡＶコンテンツを暗号化するための暗号化鍵を生成する暗号化鍵生成手段と、

ＡＶコンテンツを入力するとともに、前記暗号化鍵生成

手段からの前記暗号化鍵を入力し、その暗号化鍵を利用して、前記ＡＶコンテンツを暗号化する暗号化手段と、ＡＶコンテンツ受信装置との間で認証・鍵交換を行う送信側認証・鍵交換手段とを備え、

ＡＶコンテンツ送信装置が、前記暗号化手法選択手段によって選択された第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、

その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置から認証要求があると、前記送信側認証・鍵交換手段は、その認証要求をしたＡＶコンテンツ受信装置との間で認証を行い、

前記暗号化手法選択手段は、暗号化手法を、前記認証要求をしたＡＶコンテンツ受信装置が使用することができる第２の暗号化手法に切り替えることを特徴とするＡＶコンテンツ送信装置。

【請求項１５】前記認証要求があったさい、既にそれまでの前記第１の暗号化手法で暗号化されたＡＶコンテンツを受信し解読していた、前記認証要求をしたＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置がある場合、

その別のＡＶコンテンツ受信装置に、暗号化手法が前記第２の暗号化手法に切り替わることを通知する暗号化手法通知手段を備えたことを特徴とする請求項１４記載のＡＶコンテンツ送信装置。

【請求項１６】前記暗号化鍵生成手段は、定期的または不定期に前記暗号化鍵を更新し、

前記暗号化手法選択手段が暗号化手法を前記第２の暗号化手法に切り替えるタイミングは、前記暗号化鍵生成手段が前記第１の暗号化手法において暗号化鍵を更新するタイミングであることを特徴とする請求項１４記載のＡＶコンテンツ送信装置。

【請求項１７】前記送信側認証・鍵交換手段は、前記認証要求をしたＡＶコンテンツ受信装置を記憶するとともに、そのＡＶコンテンツ受信装置から、前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなると判断した場合、前記暗号化手法選択手段は、前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替えることを特徴とする請求項１４記載のＡＶコンテンツ送信装置。

【請求項１８】前記送信側認証・鍵交換手段は、前記認証要求をしたＡＶコンテンツ受信装置と前記そのＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、

前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドを送信してくるＡＶコンテンツ受信装置が、全て前記第１の暗号化手法を使用することができるＡＶコンテンツ受信装置である場

合、

前記暗号化手法選択手段は、前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替えることを特徴とする請求項１４記載のＡＶコンテンツ送信装置。

【請求項１９】請求項１４から１８のいずれかに記載のＡＶコンテンツ送信装置との間で認証・鍵交換を行う受信側認証・鍵交換手段と、

前記ＡＶコンテンツ送信装置からの暗号化されたＡＶコンテンツのその暗号化に利用された暗号化手法の情報を

入力し、記憶する暗号化手法記憶手段と、前記ＡＶコンテンツ送信装置からの暗号化されたＡＶコンテンツを入力するとともに、前記ＡＶコンテンツ送信装置からの暗号化鍵またはその暗号化鍵の種を入力し、その後、前記暗号化手法記憶手段に記憶されている暗号化手法に基づき、かつ、前記暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたＡＶコンテンツを解読する暗号解読手段とを備えたことを特徴とするＡＶコンテンツ受信装置。

【請求項２０】請求項１４から１８のいずれかに記載のＡＶコンテンツ送信装置から送信されてくるＡＶコンテンツとともに、またはそのＡＶコンテンツのなかに、前記暗号化手法の切り替えに関する情報があって、

その情報に、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種との一方または両方が含まれていない場合、

前記ＡＶコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記情報に含まれていないものを送信するように要求する要求手段を備えたことを特徴とする請求項１９記載のＡＶコンテンツ受信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、異なる暗号化手法で暗号化されたＡＶコンテンツの送信と、そのＡＶコンテンツの受信とに関するものである。

【０００２】

【従来の技術】近年、映画等のＡＶコンテンツをデジタル信号を用いて送信し、そのＡＶコンテンツを受信するといったことに関する技術が進歩してきている。

【０００３】そのようなＡＶコンテンツを送信する送信装置は、ＡＶコンテンツを送信する前に、内容を保護するという目的のために、ＡＶコンテンツの暗号化を行う。そして、受信装置は、暗号化されたＡＶコンテンツを受信し解読して、そのＡＶコンテンツの内容をモニタに表示する。

【０００４】さて、上述したように、送信装置はＡＶコンテンツを暗号化するが、その暗号化に用いる暗号化手

法には、複数の種類がある。例えば、受信装置がテレビ等の通常の家電機器であれば、そのような家電機器に対応させて、M6、Blowfish等の'baseline cipher'と呼ばれる「基本暗号化手法」が用いられる。それに対して、例えば、受信装置がパソコン等の演算能力の高い機器であれば、DES等の暗号の強度がより高く、より複雑な「拡張暗号化手法」が用いられる。

【0005】

【発明が解決しようとする課題】ところで、送信装置がパソコン等の演算能力の高い機器であって、IEEE 1394バスを利用して、AVコンテンツを送信し、そのIEEE 1394バスを介して、受信装置がAVコンテンツを受信する場合、上述したように、受信装置がパソコン等の演算能力の高い機器であれば、送信装置は「拡張暗号化手法」を使用してAVコンテンツを暗号化し送信しても、受信装置はそのAVコンテンツを解読することができるので、何等問題は起こらない。

【0006】しかしながら、図6に示すように、例えば、パソコン28という受信装置とともに、セットトップボックス（衛星放送受信機）29のような通常の家電機器も、IEEE 1394バスを介して送信装置27に接続されている場合がある。その場合、送信装置27が「拡張暗号化手法」を使用してAVコンテンツを暗号化して送信し、パソコン28が受信し解読しているときに、その送信の途中から、セットトップボックス29がそのAVコンテンツを受信し解読しようとしても、セットトップボックス29は、「拡張暗号化手法」を使用することができないので、そのAVコンテンツを解読することができない。

【0007】本発明は、上述したように、AVコンテンツ送信装置が第1の暗号化手法で暗号化したAVコンテンツを送信しているときに、その第1の暗号化手法を使用することができないAVコンテンツ受信装置がそのAVコンテンツを解読することができないという課題を考慮して、AVコンテンツ送信装置が第1の暗号化手法で暗号化したAVコンテンツを送信しているときに、その第1の暗号化手法を使用することができないAVコンテンツ受信装置がそのAVコンテンツを解読することができるようにするAVコンテンツ送信方法を提供することを目的とするものである。

【0008】また、本発明は、第1の暗号化手法で暗号化したAVコンテンツを送信しているときに、その第1の暗号化手法を使用することができないAVコンテンツ受信装置がそのAVコンテンツを解読することができるようにするAVコンテンツ送信装置を提供することを目的とするものである。

【0009】また、本発明は、上述したAVコンテンツ送信方法を用いたさい、第1の暗号化手法で暗号化されたAVコンテンツを受信し解読していた、第1の暗号化手法を使用することができないAVコンテンツ受信装置

とは別のAVコンテンツ受信装置がある場合、その別のAVコンテンツ受信装置が引き続きそのAVコンテンツを解読することができるようにするAVコンテンツ送信方法およびAVコンテンツ受信方法を提供することを目的とするものである。

【0010】さらに、本発明は、上述したAVコンテンツ送信装置が第1の暗号化手法を使用することができないAVコンテンツ受信装置にそのAVコンテンツを解読させる場合、そのAVコンテンツ受信装置とは別に、第1の暗号化手法で暗号化されていたAVコンテンツを引き続き解読するAVコンテンツ受信装置を提供することを目的とするものである。

【0011】

【課題を解決するための手段】第1の本発明（請求項1に対応）は、AVコンテンツ送信装置が伝送路を利用して第1の暗号化手法で暗号化したAVコンテンツを送信しているときに、その第1の暗号化手法を使用することができないAVコンテンツ受信装置から認証要求があると、その認証要求をしたAVコンテンツ受信装置が使用することができる第2の暗号化手法で前記AVコンテンツを暗号化して送信することを特徴とするAVコンテンツ送信方法である。

【0012】第2の本発明（請求項2に対応）は、第1の本発明のAVコンテンツ送信方法において、前記認証要求があったさい、既にそれまでの前記第1の暗号化手法で暗号化されたAVコンテンツを受信し解読していた、前記認証要求をしたAVコンテンツ受信装置とは別のAVコンテンツ受信装置がある場合、その別のAVコンテンツ受信装置に、暗号化手法が前記第2の暗号化手法に切り替わることを通知することを特徴とするAVコンテンツ送信方法である。

【0013】第3の本発明（請求項3に対応）は、第2の本発明のAVコンテンツ送信方法において、前記暗号化手法の切り替えを、所定のコマンドを用いて、または前記AVコンテンツのなかに付加して通知することを特徴とするAVコンテンツ送信方法である。

【0014】第4の本発明（請求項4に対応）は、第3の本発明のAVコンテンツ送信方法において、前記切り替えた後の前記第2の暗号化手法がどのような暗号化手法であるのかという情報を、所定のコマンドを用いて、または前記AVコンテンツのなかに付加して通知することを特徴とするAVコンテンツ送信方法である。

【0015】第5の本発明（請求項5に対応）は、第3の本発明のAVコンテンツ送信方法において、前記切り替えた後の前記第2の暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を、所定のコマンドを用いて、または前記AVコンテンツのなかに付加して通知することを特徴とするAVコンテンツ送信方法である。

【0016】第6の本発明（請求項6に対応）は、第1の本発明のAVコンテンツ送信方法において、前記暗号

化手法の切り替えのタイミングを、前記認証要求がある前に使用していた前記第1の暗号化手法での暗号化鍵の更新のタイミングとすることを特徴とするAVコンテンツ送信方法である。

【0017】第7の本発明（請求項7に対応）は、第2の本発明のAVコンテンツ送信方法において、少なくとも前記別のAVコンテンツ受信装置に、前記暗号化手法が前記第2の暗号化手法に切り替わることを通知するとともに、その暗号化手法の切り替えのタイミングの情報を送信することを特徴とするAVコンテンツ送信方法である。

【0018】第8の本発明（請求項8に対応）は、第1の本発明のAVコンテンツ送信方法において、前記AVコンテンツ送信装置が前記認証要求をしたAVコンテンツ受信装置を記憶し、そのAVコンテンツ受信装置から、前記AVコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなった場合、前記暗号化手法を前記第2の暗号化手法から前記第1の暗号化手法に切り替えることを特徴とするAVコンテンツ送信方法である。

【0019】第9の本発明（請求項9に対応）は、第1の本発明のAVコンテンツ送信方法において、前記AVコンテンツ送信装置が、前記認証要求をしたAVコンテンツ受信装置と前記そのAVコンテンツ受信装置とは別のAVコンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、前記AVコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドを送信してくるAVコンテンツ受信装置が、全て前記第1の暗号化手法を使用することができるAVコンテンツ受信装置である場合、前記暗号化手法を前記第2の暗号化手法から前記第1の暗号化手法に切り替えることを特徴とするAVコンテンツ送信方法である。

【0020】第10の本発明（請求項10に対応）は、第1から第9のいずれかの本発明のAVコンテンツ送信方法の各ステップの全部または一部を実現するためのプログラムを格納したことを特徴とする媒体である。

【0021】第11の本発明（請求項11に対応）は、第1から第9のいずれかの本発明のAVコンテンツ送信方法によって送信されてくるAVコンテンツを受信し、そのAVコンテンツが暗号化されたさいに使用された暗号化手法に基づくとともに、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたAVコンテンツを解読することを特徴とするAVコンテンツ受信方法である。

【0022】第12の本発明（請求項12に対応）は、第11の本発明のAVコンテンツ送信方法において、第1から第9のいずれかの本発明のAVコンテンツ送信方

法によって送信されてくるAVコンテンツとともに、またはそのAVコンテンツのなかに、前記暗号化手法の切り替えに関する情報があって、その情報に、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種との一方または両方が含まれていない場合、前記AVコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記暗号化手法の切り替えに関する情報に含まれていないものを送信するように要求することを特徴とするAVコンテンツ受信方法である。

【0023】第13の本発明（請求項13に対応）は、第11または第12の本発明のAVコンテンツ受信方法の各ステップの全部または一部を実現するためのプログラムを格納したことを特徴とする媒体である。

【0024】第14の本発明（請求項14に対応）は、送信しようとするAVコンテンツを暗号化するさいの暗号化手法を選択する暗号化手法選択手段と、その暗号化手法選択手段によって選択された暗号化手法に対応した、AVコンテンツを暗号化するための暗号化鍵を生成する暗号化鍵生成手段と、AVコンテンツを入力するとともに、前記暗号化鍵生成手段からの前記暗号化鍵を入力し、その暗号化鍵を利用して、前記AVコンテンツを暗号化する暗号化手段と、AVコンテンツ受信装置との間で認証・鍵交換を行う送信側認証・鍵交換手段とを備え、AVコンテンツ送信装置が、前記暗号化手法選択手段によって選択された第1の暗号化手法で暗号化したAVコンテンツを送信しているときに、その第1の暗号化手法を使用することができないAVコンテンツ受信装置から認証要求があると、前記送信側認証・鍵交換手段が、その認証要求をしたAVコンテンツ受信装置との間で認証を行い、前記暗号化手法選択手段が、暗号化手法を、前記認証要求をしたAVコンテンツ受信装置が使用することができる第2の暗号化手法に切り替えることを特徴とするAVコンテンツ送信装置である。

【0025】第15の本発明（請求項15に対応）は、第14の本発明のAVコンテンツ送信装置において、前記認証要求があったさい、既にそれまでの前記第1の暗号化手法で暗号化されたAVコンテンツを受信し解読していた、前記認証要求をしたAVコンテンツ受信装置とは別のAVコンテンツ受信装置がある場合、その別のAVコンテンツ受信装置に、暗号化手法が前記第2の暗号化手法に切り替わることを通知する暗号化手法通知手段を備えたことを特徴とするAVコンテンツ送信装置である。

【0026】第16の本発明（請求項16に対応）は、第14の本発明のAVコンテンツ送信装置において、前記暗号化鍵生成手段が、定期的または不定期に前記暗号

化鍵を更新し、前記暗号化手法選択手段が暗号化手法を前記第2の暗号化手法に切り替えるタイミングが、前記暗号化鍵生成手段が前記第1の暗号化手法において暗号化鍵を更新するタイミングであることを特徴とするAVコンテンツ送信装置である。

【0027】第17の本発明（請求項17に対応）は、第14の本発明のAVコンテンツ送信装置において、前記送信側認証・鍵交換手段が、前記認証要求をしたAVコンテンツ受信装置を記憶するとともに、そのAVコンテンツ受信装置から、前記AVコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなったと判断した場合、前記暗号化手法選択手段が、前記暗号化手法を前記第2の暗号化手法から前記第1の暗号化手法に切り替えることを特徴とするAVコンテンツ送信装置である。

【0028】第18の本発明（請求項18に対応）は、第14の本発明のAVコンテンツ送信装置において、前記送信側認証・鍵交換手段が、前記認証要求をしたAVコンテンツ受信装置と前記そのAVコンテンツ受信装置とは別のAVコンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、前記AVコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドを送信してくるAVコンテンツ受信装置が、全て前記第1の暗号化手法を使用することができるAVコンテンツ受信装置である場合、前記暗号化手法選択手段が、前記暗号化手法を前記第2の暗号化手法から前記第1の暗号化手法に切り替えることを特徴とするAVコンテンツ送信装置である。

【0029】第19の本発明（請求項19に対応）は、第14から第18のいずれかの本発明のAVコンテンツ送信装置との間で認証・鍵交換を行う受信側認証・鍵交換手段と、前記AVコンテンツ送信装置からの暗号化されたAVコンテンツのその暗号化に利用された暗号化手法の情報を入力し、記憶する暗号化手法記憶手段と、前記AVコンテンツ送信装置からの暗号化されたAVコンテンツを入力するとともに、前記AVコンテンツ送信装置からの暗号化鍵またはその暗号化鍵の種を入力し、その後、前記暗号化手法記憶手段に記憶されている暗号化手法に基づき、かつ、前記暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたAVコンテンツを解読する暗号解読手段とを備えたことを特徴とするAVコンテンツ受信装置である。

【0030】第20の本発明（請求項20に対応）は、第19の本発明のAVコンテンツ受信装置において、第14から第18のいずれかの本発明のAVコンテンツ送信装置から送信されてくるAVコンテンツとともに、またはそのAVコンテンツのなかに、前記暗号化手法の切り替えに関する情報があって、その情報に、前記切り替

え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種との一方または両方が含まれていない場合、前記AVコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記情報に含まれていないものを送信するように要求する要求手段を備えたことを特徴とするAVコンテンツ受信装置である。

【0031】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。

【0032】（実施の形態1）まず、本発明の実施の形態1のAVコンテンツ通信システムの構成を述べる。

【0033】図1に、本発明の実施の形態1のAVコンテンツ通信システムのブロック図を示す。図1に示すように、本発明の実施の形態1のAVコンテンツ通信システムは、AVコンテンツ送信装置1と、第1のAVコンテンツ受信装置2と、第2のAVコンテンツ受信装置3と、IEEE1394バスから構成される。なお、図1には、アンテナ4と、モニタ5および6も表示する。

【0034】さて、AVコンテンツ送信装置1は、図1に示すように、受信手段7と、暗号化手段8と、Kc o生成手段9と、暗号化手法選択手段10と、AKE手段11と、暗号化手法変更通知手段12と、Kc o要求コマンド応答手段13と、データ転送手段14から構成される。

【0035】受信手段7は、AVコンテンツを、AVコンテンツ送信装置1外部のアンテナ4を介して受信する手段である。

【0036】暗号化手段8は、基本暗号化手法と拡張暗号化手法とを使用することができるものであって、受信手段7からのAVコンテンツを入力するとともに、Kc o生成手段9からの暗号化鍵Kc oを入力し、暗号化手法選択手段10によって選択された暗号化手法を使用し、暗号化鍵Kc oでAVコンテンツを暗号化する手段である。なお、暗号化鍵Kc oで暗号化されたAVコンテンツをKc o（AVコンテンツ）とする。また、基本暗号化手法と拡張暗号化手法との相違は、暗号化の強度が異なるということであって、拡張暗号化手法の方が基本暗号化手法よりも暗号化の強度が強いものであるとする。さらにいうと、暗号化するさいに用いる暗号化鍵Kc oを構成するデジタル信号の長さが異なり、例えば、基本暗号化手法は、40ビットの暗号化鍵Kc oを用いてAVコンテンツを暗号化する手法であって、拡張暗号化手法は、56ビットの暗号化鍵Kc oを用いてAVコンテンツを暗号化する手法であるものとする。

【0037】Kc o生成手段9は、暗号化手段8が受信手段7からのAVコンテンツを暗号化するさいに用いる暗号化鍵Kc oを生成する手段であって、その暗号化鍵

K c oを20秒毎に更新するものである。

【0038】暗号化手法選択手段10は、暗号化手段8がAVコンテンツを暗号化するさいに使用する暗号化手法を選択する手段である。

【0039】AKE手段11は、第1のAVコンテンツ受信装置2との間で認証・鍵交換を行う手段であって、第1のAVコンテンツ受信装置2との間で認証が成功した場合、その第1のAVコンテンツ受信装置2に対して、交換鍵K e x (ExchangeKey)を発行する手段である。また同様に、AKE手段11は、第2のAVコンテンツ受信装置3との間で認証・鍵交換を行う手段でもある。

【0040】暗号化手法変更通知手段12は、それまでに選択していた暗号化手法からそれとは別の暗号化手法に暗号化手法の選択を変更する場合、その変更を通知する手段である。

【0041】K c o要求コマンド応答手段13は、第1のAVコンテンツ受信装置2および/または第2のAVコンテンツ受信装置3からの、20秒毎に更新される最新の暗号化鍵K c oの種を送信するように要求されたコマンドを入力し、そのコマンドにしたがって暗号化鍵K c oの種を送信する手段である。

【0042】データ転送手段14は、AVコンテンツ送信装置1の各構成手段と第1のAVコンテンツ受信装置2および/または第2のAVコンテンツ受信装置3との間でのデータ通信の仲介を行う手段である。

【0043】次に、第1のAVコンテンツ受信装置2は、図1に示すように、データ転送手段15と、AKE手段16と、暗号化手法通知検出手段17と、K c o要求コマンド発行手段18と、K c o記憶手段19と、暗号化手法記憶手段20と、暗号解読手段21から構成される。

【0044】データ転送手段15は、第1のAVコンテンツ受信装置2の各構成手段とAVコンテンツ送信装置1との間でのデータ通信の仲介を行う手段である。

【0045】AKE手段16は、AVコンテンツ送信装置1との間で認証・鍵交換を行う手段であって、AVコンテンツ送信装置1との間で認証が成功した場合、そのAVコンテンツ送信装置1から交換鍵K e xを入力する手段である。

【0046】暗号化手法通知検出手段17は、AVコンテンツ送信装置1からのAVコンテンツの暗号化に使用された暗号化手法がどのような暗号化手法であるのかを検出する手段である。

【0047】K c o要求コマンド発行手段18は、暗号化手法通知検出手段17によって検出された暗号化手法にしたがって、その暗号化手法に対応する暗号化鍵K c oの種を送信するようにAVコンテンツ送信装置1に対して要求するコマンドを発行する手段である。また、K c o要求コマンド発行手段18は、その要求コマンドに

対応する、AVコンテンツ送信装置1からの暗号化鍵K c oの種を入力する手段でもある。

【0048】K c o記憶手段19は、あらかじめ、AVコンテンツ送信装置1からの暗号化されたAVコンテンツを解読するさいに必要となる所定の関数が設定されており、AKE手段16からの交換鍵K e xを入力するとともに、K c o要求コマンド発行手段18からの暗号化鍵K c oの種を入力し、交換鍵K e xと暗号化鍵K c oとをあらかじめ設定されている関数に代入して暗号化鍵K c oを生成し記憶する手段である。なお、その関数については後に述べることにする。

【0049】暗号化手法記憶手段20は、暗号化手法通知検出手段17によって検出された暗号化手法を記憶する手段である。

【0050】暗号解読手段21は、AVコンテンツ送信装置1からの暗号化されたAVコンテンツを入力するとともに、K c o記憶手段19からの暗号化鍵K c oと、暗号化手法記憶手段20からの暗号化手法とを入力し、その暗号化手法に基づいて、暗号化されたAVコンテンツを暗号化鍵K c oで解読する手段である。なお、暗号解読手段21は、基本暗号化手法と拡張暗号化手法のいずれもを使用することができるものであるとする。

【0051】次に、第2のAVコンテンツ受信装置3は、図1に示すように、データ転送手段22と、AKE手段23と、K c o要求コマンド発行手段24と、K c o記憶手段25と、暗号解読手段26から構成される。

【0052】データ転送手段22は、第2のAVコンテンツ受信装置3の各構成手段とAVコンテンツ送信装置1との間でのデータ通信の仲介を行う手段である。

【0053】AKE手段23は、AVコンテンツ送信装置1との間で認証・鍵交換を行う手段であって、AVコンテンツ送信装置1との間で認証が成功した場合、そのAVコンテンツ送信装置1から交換鍵K e xを入力する手段である。

【0054】K c o要求コマンド発行手段24は、基本暗号化手法に対応する暗号化鍵K c oの種を送信するようにAVコンテンツ送信装置1に対して要求するコマンドを発行する手段である。また、K c o要求コマンド発行手段24は、その要求コマンドに対応する、AVコンテンツ送信装置1からの最新の暗号化鍵K c oの種を入力する手段でもある。

【0055】K c o記憶手段26は、あらかじめ、AVコンテンツ送信装置1からの暗号化されたAVコンテンツを解読するさいに必要となる所定の関数が設定されており、AKE手段23からの交換鍵K e xを入力するとともに、K c o要求コマンド発行手段24からの暗号化鍵K c oの種を入力し、交換鍵K e xと暗号化鍵K c oとをあらかじめ設定されている関数に代入して暗号化鍵K c oを生成し記憶する手段である。

【0056】暗号解読手段26は、AVコンテンツ送信

装置1からの暗号化されたAVコンテンツを入力するとともに、Kc o記憶手段25からの暗号化鍵Kc oを入力し、基本暗号化手法に基づいて、暗号化されたAVコンテンツを暗号化鍵Kc oで解読する手段である。なお、暗号解読手段26は、基本暗号化手法のみを使用することができるものであるとする。いいかえると、暗号解読手段26は、拡張暗号化手法を使用することができないものである。

【0057】次に、IEEE1394バスは、AVコンテンツ送信装置1、第1のAVコンテンツ受信装置2および第2のAVコンテンツ受信装置3それぞれの間で通信されるデータの伝送路である。

【0058】また、アンテナ4は、AVコンテンツ送信装置1外部に設置され、AVコンテンツを受信する手段である。モニタ5は、第1のAVコンテンツ受信装置2からのAVコンテンツを表示する手段であり、同様に、モニタ6は、第2のAVコンテンツ受信装置3からのAVコンテンツを表示する手段である。

【0059】次に、本発明の実施の形態1のAVコンテンツ通信システムの動作を述べる。

【0060】図1のAVコンテンツ通信システムの動作を詳しく述べる前に、以下の説明の便宜上、次に示す状況を想定し、その状況下でのAVコンテンツ通信システムの動作を述べることにする。

【0061】その状況とは、先ず、AVコンテンツ送信装置1がアンテナ4からのAVコンテンツを拡張暗号化手法を用いて暗号化してIEEE1394バスに出力しており、そのAVコンテンツの出力の途中から、第1のAVコンテンツ受信装置2がそのAVコンテンツを受信して解読し、さらにその後、拡張暗号化手法を使用することができない第2のAVコンテンツ受信装置3がそのAVコンテンツを受信して解読しようとする状況である。

【0062】さて、はじめに、AVコンテンツ送信装置1がアンテナ4からのAVコンテンツを拡張暗号化手法を用いて暗号化しIEEE1394バスに出力するまでのAVコンテンツ送信装置1の動作を述べる。なお、AVコンテンツ送信装置1は、上述したように、拡張暗号化手法を使用することもできるし、基本暗号化手法を使用することもできるが、出力するAVコンテンツの内容をより強く保護するという目的のために、基本暗号化手法を使用して暗号化したAVコンテンツを出力するようにを要求されることがなければ、暗号化強度のより強い拡張暗号化手法を使用してAVコンテンツを暗号化するものとする。

【0063】先ず、暗号化手法選択手段10は、拡張暗号化手法を選択し、受信手段7は、AVコンテンツ送信装置1外部のアンテナ4を介してAVコンテンツを受信し、暗号化手段8は、受信手段7からのAVコンテンツを入力するとともに、Kc o生成手段9からの暗号化鍵

Kc o1を入力し、その後、拡張暗号化手法に基づいて、暗号化鍵Kc o1でAVコンテンツを暗号化する。なお、Kc o生成手段9からの暗号化鍵を、拡張暗号化手法に対応する暗号化鍵であることを示すために、「Kc o1」というように記述した。また、以下では、その拡張暗号化手法とは別の基本暗号化手法に対応する暗号化鍵を「Kc o2」というように記述する。ところで、暗号化は、例えばAVコンテンツの一部のヘッダについては行われないものとする。つまり、AVコンテンツが受信されたさいに、暗号化鍵Kc o1がなくてもそのAVコンテンツのヘッダ情報は解読されるが、そのAVコンテンツの内容は暗号化鍵Kc o1がなくては解読されないように暗号化が行われるものとする。また、暗号化手段8が利用するKc o生成手段9からの暗号化鍵Kc o1は、上述したように20秒毎に更新されるものとする。そして、Kc o生成手段9は、暗号化鍵Kc o1がどのタイミングで更新するのかという情報として、oddまたはevenを出力する。そのoddまたはevenは、互いに相手方から切り替わったときに、その切り替わりの前後でAVコンテンツの暗号化に使用された暗号化鍵Kc o1が20秒毎の更新により切り替わっていることを示すためのものであるとする。その後、データ転送手段14は、暗号化手段8からの暗号化鍵Kc o1で暗号化されたAVコンテンツ、つまりKc o (AVコンテンツ)を入力するとともに、Kc o生成手段9からのoddまたはevenを入力し、図2(a)に示すように、Kc o (AVコンテンツ)のヘッダのなかにoddまたはevenを付加してIEEE1394バスに出力する。なお、図2(a)は、AVコンテンツ送信装置1から送信されるAVコンテンツの構成図である。図2(b)については後に説明する。

【0064】次に、上述したようにしてAVコンテンツ送信装置1がAVコンテンツを暗号化してIEEE1394バスに出力しているときに、その途中から、第1のAVコンテンツ受信装置2がそのAVコンテンツを解読するところまでのAVコンテンツ送信装置1と第1のAVコンテンツ受信装置2の動作を述べる。

【0065】このとき、第1のAVコンテンツ受信装置2のAKE手段16は、AVコンテンツ送信装置1のAKE手段11に対して、認証要求を行い、AKE手段16およびAKE手段11は、互いに相手方の装置の認証を行う。その認証が成功すると、AKE手段11は、AKE手段16に交換鍵Kexを出力する。その交換鍵Kexは、暗号化されたAVコンテンツを解読するさいに必要な鍵である。それとともに、AKE手段11は、第1のAVコンテンツ受信装置2が拡張暗号化手法を使用することができるものであることを判断し、暗号化手法の変更を行わない。なお、AKE手段16およびAKE手段11が行う認証が失敗した場合、AKE手段11は、AKE手段16に交換鍵Kexを出力すること

はない。ここでは、以下の説明の便宜上、AKE手段16およびAKE手段11が行う認証は成功するものとする。そして、第1のAVコンテンツ受信装置2のAKE手段16は、データ転送手段15を介して、AKE手段11からの交換鍵 K_{ex} を入力し、 K_{co} 記憶手段19に出力する。また、暗号化手法通知検出手段17は、AVコンテンツ送信装置1からのAVコンテンツが拡張暗号化手法で暗号化されたものであることを検出し、その旨の情報、つまり拡張暗号化手法を暗号化手法記憶手段20に出力し記憶させる。さらに、 K_{co} 要求コマンド発行手段18は、拡張暗号化手法に対応する最新の暗号化鍵 $K_{co}1$ の種を送信するように、AVコンテンツ送信装置1の K_{co} 要求コマンド応答手段13に対してコマンドを発行し、そのコマンドに対応する K_{co} 要求コマンド応答手段13からの最新の暗号化鍵 $K_{co}1$ の種を入力して、その種を K_{co} 記憶手段19に出力する。なお、上述したように、AVコンテンツ送信装置1からの暗号化鍵 $K_{co}1$ が20秒毎に更新されるので、 K_{co} 要求コマンド発行手段18は、 K_{co} 要求コマンド応答手段13に対するコマンドを20秒毎に発行するものとする。その後、 K_{co} 記憶手段19は、後述する(数1)に示すように、あらかじめ設定されている関数に、AKE手段16からの交換鍵 K_{ex} と、 K_{co} 要求コマンド発行手段18からの暗号化鍵 $K_{co}1$ の種とを代入し、暗号化鍵 $K_{co}1$ を生成し記憶する。ただし、(数1)の $seed$ のところに、暗号化鍵 $K_{co}1$ の種を代入する。

【0066】

【数1】 $K_{co} = f(seed, K_{ex})$

そして、AVコンテンツ送信装置1からの K_{co} (AVコンテンツ)のヘッダのなかの odd または $even$ を検出し、さらに、 odd と $even$ との切り替わりを判断して、AVコンテンツ送信装置1からの K_{co} (AVコンテンツ)がどの暗号化鍵 $K_{co}1$ で暗号化されたのかを特定する。なお、上述したように、 odd と $even$ との切り替わりは、その切り替わりの前後でAVコンテンツの暗号化に使用された暗号化鍵 $K_{co}1$ が切り替わっていることを示す。また、AVコンテンツ送信装置1の K_{co} 要求コマンド応答手段13は、 K_{co} 要求コマンド発行手段18からの、暗号化鍵 $K_{co}1$ の種の送信要求のコマンドを入力すると、そのコマンドにしたがって、暗号化鍵 $K_{co}1$ の種をデータ転送手段14に出力する。そして、データ転送手段14は、図2に示すように、 K_{co} (AVコンテンツ)に使用した暗号化鍵 $K_{co}1$ の種を、 K_{co} (AVコンテンツ)とは別の非同期信号を使用してコマンドでIEEE1394バスに出力する。なお、図2(b)は、AVコンテンツ送信装置1から送信されるコマンドの構成図である。

【0067】最後に、暗号解読手段21は、AVコンテンツ送信装置1からの暗号化されたAVコンテンツをデ

ータ転送手段15を介して入力するとともに、 K_{co} 記憶手段19からの暗号化鍵 $K_{co}1$ と、暗号化手法記憶手段20からの拡張暗号化手法とを入力し、その拡張暗号化手法に基づいて、暗号化されたAVコンテンツを暗号化鍵 $K_{co}1$ で解読し、モニタ5に出力する。そして、モニタ5は、暗号解読手段21からのAVコンテンツの内容を表示する。

【0068】次に、上述したようにして、AVコンテンツ送信装置1が拡張暗号化手法を使用してAVコンテンツを暗号化して出力し、第1のAVコンテンツ受信装置2がそのAVコンテンツを解読しているときに、拡張暗号化手法を使用することができない第2のAVコンテンツ受信装置3がそのAVコンテンツを解読するさいのAVコンテンツ送信装置1、第1のAVコンテンツ受信装置2および第2のAVコンテンツ受信装置3の動作を述べる。なお、そのさいのAVコンテンツ送信装置1の動作については図3のフローチャートをも用いて説明する。

【0069】さて、第2のAVコンテンツ受信装置3のAKE手段23は、AVコンテンツ送信装置1のAKE手段11に対して、認証要求を行い、AKE手段23およびAKE手段11は、互いに相手方の装置の認証を行う(図3のステップ1)。そのさい、AKE手段23は、AVコンテンツ送信装置1が出力するAVコンテンツの暗号化手法を、基本暗号化手法にするように要求する。なぜなら、第2のAVコンテンツ受信装置3は、拡張暗号化手法を使用することができず、基本暗号化手法しか使用することができないからである。そして、互いの認証が成功すると、AKE手段11は、その要求を受け入れ(図3のステップ2)、暗号化手法選択手段10および暗号化手法変更通知手段12に、暗号化手法を基本暗号化手法にするように制御するための情報を出力する(図3のステップ3)。その後、AKE手段11は、AKE手段23に交換鍵 K_{ex} を出力し、AKE手段11とAKE手段23との間の認証・鍵交換は完了する(図3のステップ4)。なお、交換鍵 K_{ex} は、暗号化されたAVコンテンツを解読するさいに必要となる鍵である。また、AKE手段23およびAKE手段11が行う認証が失敗した場合、AKE手段11は、AKE手段23に交換鍵 K_{ex} を出力することもないし、暗号化手法を基本暗号化手法にするようにとの要求を受け入れることもない。ただしここでは、以下の説明の便宜上、AKE手段23およびAKE手段11が行う認証は成功するものとする。

【0070】そして、AVコンテンツ送信装置1では、暗号化手法選択手段10が、AKE手段11からの、暗号化手法を基本暗号化手法にするための情報、つまり暗号化手法を変更させるための情報にしたがって、基本暗号化手法を選択し、その旨の情報を、暗号化手段8と K_{co} 生成手段9とに出力する。なお、暗号化手法選択手

段10は、AKE手段11とAKE手段23との間の認証・鍵交換が完了するまでに、いいかえると、AKE手段23が交換鍵Kexを入力するまでに、基本暗号化手法を選択する。その後、Kco生成手段9は、その暗号化手法の基本暗号化手法への変更の情報を入力した後であって、かつ、拡張暗号化手法にしたがって生成していた暗号化鍵Kco1の次の更新タイミングから、基本暗号化手法にしたがった暗号化鍵Kco2を生成し、20秒毎に更新してゆく。また、暗号化手法変更通知手段12は、AVコンテンツの暗号化手法を拡張暗号化手法から基本暗号化手法に変更するという旨の情報のコマンドを、第1のAVコンテンツ受信装置2の暗号化手法通知検出手段17に出力するとともに、その暗号化手法の切り替えのタイミングの情報のコマンドを暗号化手法通知検出手段17に出力する。

【0071】その後、AVコンテンツ送信装置1の暗号化手段8は、受信手段7からのAVコンテンツを入力するとともに、Kco生成手段9からの暗号化鍵Kco2を入力し、基本暗号化手法に基づいて、暗号化鍵Kco2でAVコンテンツを暗号化する。さらに、Kco生成手段9は、暗号化鍵Kco2がどのタイミングで切り替わるのかという情報としてoddまたはevenを出力する。そして、データ転送手段14は、暗号化手段8からの暗号化鍵Kco2で暗号化されたAVコンテンツ、つまりKco(AVコンテンツ)を入力するとともに、Kco生成手段9からのoddまたはevenを入力し、Kco(AVコンテンツ)のヘッダのなかにoddまたはevenを付加してIEEE1394バスに出力する。

【0072】このようにAVコンテンツ送信装置1からのAVコンテンツの暗号化手法が基本暗号化手法に切り替わると、第2のAVコンテンツ受信装置3は、そのAVコンテンツを解読することができるようになる。そこで次に、このときの第2のAVコンテンツ受信装置3がAVコンテンツを解読するさいの動作を述べる。

【0073】先ず、AKE手段23は、AVコンテンツ送信装置1のAKE手段11からの交換鍵Kexを、データ転送手段22を介して入力し、Kco記憶手段25に出力する。また、Kco要求コマンド発行手段24は、基本暗号化手法に対応する暗号化鍵Kco2の種を送信するように、AVコンテンツ送信装置1のKco要求コマンド応答手段13に対してコマンドを発行し、そのコマンドに対応する、Kco要求コマンド応答手段13からの暗号化鍵Kco2の種を入力して、その種をKco記憶手段25に出力する。その後、Kco記憶手段25は、(数1)を用いて上述したようにして、あらかじめ設定されている関数に、AKE手段23からの交換鍵Kexと、Kco要求コマンド発行手段24からの暗号化鍵Kco2の種とを代入し、暗号化鍵Kco2を生成し記憶する。そして、AVコンテンツ送信装置1から

のKco(AVコンテンツ)のヘッダのなかのoddまたはevenを検出し、さらに、oddとevenとの切り替わりを判断して、AVコンテンツ送信装置1からのKco(AVコンテンツ)がどの暗号化鍵Kco2で暗号化されたのかを特定する。

【0074】最後に、暗号解読手段26は、AVコンテンツ送信装置1からの暗号化されたAVコンテンツをデータ転送手段22を介して入力するとともに、Kco記憶手段25からの暗号化鍵Kco2を入力し、基本暗号化手法に基づいて、暗号化されたAVコンテンツを暗号化鍵Kco2で解読し、モニタ6に出力する。そして、モニタ6は、暗号解読手段26からのAVコンテンツの内容を表示する。

【0075】このように、AVコンテンツ送信装置1がAVコンテンツの暗号化手法を基本暗号化手法に変更してAVコンテンツを暗号化し出力すると、第2のAVコンテンツ受信装置3は、そのAVコンテンツを解読することができるようになるが、それまで拡張暗号化手法によって暗号化されたAVコンテンツを受信し解読していた第1のAVコンテンツ受信装置2は、そのままでは、そのAVコンテンツを解読することができなくなる。そこで次に、AVコンテンツ送信装置1がAVコンテンツの暗号化手法を基本暗号化手法に変更した場合、第1のAVコンテンツ受信装置2がそのAVコンテンツを解読するさいの、第1のAVコンテンツ受信装置2の動作を述べる。なお、そのさいの第1のAVコンテンツ受信装置2の動作については図4のフローチャートをも用いて説明する。

【0076】さてそのとき、上述したように、第1のAVコンテンツ受信装置2の暗号化手法通知検出手段17は、AVコンテンツ送信装置1の暗号化手法変更通知手段12からの、AVコンテンツの暗号化手法が拡張暗号化手法から基本暗号化手法に変更するという旨の情報のコマンドを入力するとともに、その暗号化手法の切り替えのタイミングの情報のコマンドも入力する(図4のステップ1)。そして、暗号化手法通知検出手段17は、それら2つの情報を、Kco要求コマンド発行手段18と暗号化手法記憶手段20とに出力する。その後、Kco要求コマンド発行手段18は、基本暗号化手法に対応する暗号化鍵Kco2の種を送信するように、AVコンテンツ送信装置1のKco要求コマンド応答手段13に対してコマンドを発行し(図4のステップ2)、そのコマンドに対応する、Kco要求コマンド応答手段13からの暗号化鍵Kco2の種を入力して、その種をKco記憶手段19に出力する。その後、Kco記憶手段19は、あらかじめ設定されている関数に、AKE手段16からの交換鍵Kexと、Kco要求コマンド発行手段18からの暗号化鍵Kco2の種とを代入し、暗号化鍵Kco2を生成し記憶する(図4のステップ3)。

【0077】最後に、暗号解読手段21は、AVコンテ

ンツ送信装置1からの暗号化されたAVコンテンツをデータ転送手段15を介して入力するとともに、Kc o記憶手段19からの暗号化鍵Kc o 2と、暗号化手法記憶手段20からの基本暗号化手法とを入力する。そして、暗号解読手段21は、基本暗号化手法を使用することができるので、その基本暗号化手法に基づいて、暗号化されたAVコンテンツを暗号化鍵Kc o 2で解読し、モニタ5に出力する(図4のステップ4)。そして、モニタ5は、暗号解読手段21からのAVコンテンツの内容を表示する。

【0078】このように、AVコンテンツ送信装置1がAVコンテンツの暗号化手法を基本暗号化手法に変更した場合であっても、第1のAVコンテンツ受信装置2は、暗号化手法が基本暗号化手法に切り替わったという情報と、その切り替えのタイミングの情報とを入力することによって、基本暗号化手法によって暗号化されたAVコンテンツを解読することができるようになる。

【0079】ところで、AVコンテンツ送信装置1がAVコンテンツの暗号化手法を基本暗号化手法に変更してAVコンテンツを送信しているとき、第2のAVコンテンツ受信装置3がそのAVコンテンツを解読することを中止することがある。以下に、そのような第2のAVコンテンツ受信装置3がAVコンテンツを解読することを中止する場合のAVコンテンツ送信装置1および第1のAVコンテンツ受信装置2の動作を述べる。

【0080】さて、第2のAVコンテンツ受信装置3がAVコンテンツを解読することを中止する場合、第2のAVコンテンツ受信装置3のKc o要求コマンド発行手段24は、暗号化鍵Kc o 2の種を送信するように、AVコンテンツ送信装置1のKc o要求コマンド応答手段13に対してコマンドを発行しなくなる。つまり、Kc o要求コマンド応答手段13にとっては、Kc o要求コマンド発行手段24からのコマンドを受信しなくなるということである。このように、Kc o要求コマンド応答手段13は、Kc o要求コマンド発行手段24からのコマンドを受信しなくなると、第2のAVコンテンツ受信装置3がAVコンテンツを解読することを中止したものと判断する。そして、Kc o要求コマンド応答手段13は、第2のAVコンテンツ受信装置3がAVコンテンツを解読することを中止したことを、暗号化手法変更通知手段12に通知する。

【0081】その後、暗号化手法変更通知手段12は、Kc o要求コマンド応答手段13からの、第2のAVコンテンツ受信装置3がAVコンテンツを解読することを中止したとする情報を入力し、その情報に基づいて、暗号化手法選択手段10に対して、選択する暗号化手法を基本暗号化手法から拡張暗号化手法に切り替えさせるとともに、第1のAVコンテンツ受信装置2の暗号化手法通知検出手段17に対して、暗号化手法が基本暗号化手法から拡張暗号化手法に切り替わるという情報を、その

切り替えのタイミングの情報とともに出力する。このように、暗号化手法を拡張暗号化手法に切り替えるのは、上述したように拡張暗号化手法の方が基本暗号化手法よりも暗号化の強度が強く、不正な装置にAVコンテンツの内容を解読させないようにする防御をより強くするためである。なお、暗号化手法を基本暗号化手法から拡張暗号化手法に切り替えるさい、あらかじめAKE手段11に、第2のAVコンテンツ受信装置3が基本暗号化手法しか使用することができないということを記憶させておき、その後、暗号化手法変更通知手段12に、第2のAVコンテンツ受信装置3がAVコンテンツを解読することを中止した場合、暗号化手法を基本暗号化手法から拡張暗号化手法に切り替えるように判断させればよい。

【0082】そして、暗号化手法選択手段10は、暗号化手法の選択を基本暗号化手法から拡張暗号化手法に再度切り替える。このように暗号化手法が拡張暗号化手法に切り替えられた後のAVコンテンツ送信装置1の各構成手段は、上述した基本暗号化手法に切り替えられる前の拡張暗号化手法に基づいてAVコンテンツを暗号化し出力していたときと同じ動作を行う。

【0083】他方、第1のAVコンテンツ受信装置2では、暗号化手法通知検出手段17が、AVコンテンツ送信装置1の暗号化手法変更通知手段12からの、暗号化手法が基本暗号化手法から拡張暗号化手法に切り替わるという情報と、その切り替えのタイミングの情報とを入力する。そして、その情報にしたがって、暗号解読するさいの各構成手段が動作を切り替える。その切り替わりのタイミングは、暗号化手法が拡張暗号化手法から基本暗号化手法に切り替わったタイミングと同様に行われ、またその切り替え後の第1のAVコンテンツ受信装置2の各構成手段は、上述した基本暗号化手法に切り替えられる前の拡張暗号化手法に基づいて暗号化されたAVコンテンツを解読するさいの動作と同じように動作する。

【0084】このように、AVコンテンツ送信装置1がAVコンテンツの暗号化手法を基本暗号化手法を使用して暗号化しAVコンテンツを送信しているとき、第2のAVコンテンツ受信装置3がそのAVコンテンツを解読することを中止した場合、AVコンテンツ送信装置1は、暗号化強度のより強い拡張暗号化手法で暗号化したAVコンテンツを送信するように変更する。このように暗号化手法が基本暗号化手法から拡張暗号化手法に変更された場合であっても、第1のAVコンテンツ受信装置2は、それに対応してそのAVコンテンツを解読することができる。

【0085】なお、上述した実施の形態1では、AVコンテンツ送信装置1の暗号化手法変更通知手段12は、AVコンテンツの暗号化手法が拡張暗号化手法から基本暗号化手法に変更するという旨の情報のコマンドを第1のAVコンテンツ受信装置2の暗号化手法通知検出手段17に出力するとした。しかしながら、暗号化手法変更

通知手段12は、AVコンテンツの暗号化手法が拡張暗号化手法から他の暗号化手法に変更するという旨の情報を暗号化手法通知検出手段17に出力するとしてもよい。ただしこの場合、暗号化手法通知検出手段17は、変更後の暗号化手法がどのような暗号化手法であるのかを通知するように、AVコンテンツ送信装置1に要求しなければならない。同様に、暗号化手法変更通知手段12は、暗号化手法の拡張暗号化手法から基本暗号化手法への切り替えのタイミングの情報をコマンドで暗号化手法通知検出手段17に出力するとしたが、暗号化手法変更通知手段12は、そのような暗号化手法の切り替えのタイミングの情報を暗号化手法通知検出手段17に出力しないとしてもよい。ただしこの場合も、暗号化手法通知検出手段17は、暗号化手法の切り替えのタイミングの情報を通知するように、AVコンテンツ送信装置1に要求しなければならない。また、暗号化手法変更通知手段12が出力する暗号化手法の切り替えの情報や切り替えのタイミングの情報は、コマンドではなく、AVコンテンツのなかに付加されたものであってもよい。

【0086】また、上述した実施の形態1では、AVコンテンツ送信装置1は、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるさい、暗号化手法のみがどのような暗号化手法に切り替わるのかという情報を出力し、その後、第1のAVコンテンツ受信装置2から、その変更後の暗号化手法に対応する暗号化鍵Kc oの種を送信するように要求された場合、その要求にしたがって、暗号化鍵Kc oの種を送信するとした。しかしながら、AVコンテンツ送信装置1は、暗号化手法を切り替えるさい、切り替わった後の暗号化手法の情報とともに、その変更後の暗号化手法に対応する暗号化鍵Kc oの種を出力するとしてもよい。また、AVコンテンツ送信装置1は、暗号化鍵Kc oの種を出力するとしたが、暗号化鍵Kc oそのもの、または交換鍵Kexで暗号化した暗号化鍵Kc oを出力してもよい。その場合、受信側では、種ではなく、暗号化鍵Kc oそのもの、または交換鍵Kexで暗号化された暗号化鍵Kc oが使用されることになる。また、暗号化鍵Kc oの種はコマンドを利用して送信されることが、暗号化鍵Kc oやその種は、コマンドで送信されても、AVコンテンツのなかに付加されて送信されてもよい。

【0087】また、上述した実施の形態1では、AVコンテンツ送信装置1のKc o生成手段9は、20秒毎に暗号化鍵Kc oを更新するとしたが、Kc o生成手段9が暗号化鍵Kc oを更新する間隔は、20秒毎という間隔に限定されるものではない。暗号化鍵Kc oは、定期的に更新されてもよいし、不定期に更新されてもよい。

【0088】また、上述した実施の形態1では、AVコンテンツ送信装置1が第2のAVコンテンツ受信装置3を記憶し、その第2のAVコンテンツ受信装置3から、AVコンテンツを解読するための暗号化鍵Kc o2の種

を要求するコマンドが来ているか否かを判断し、そのコマンドが来なくなった場合、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるとした。しかしながら、AVコンテンツ送信装置1が、第1のAVコンテンツ受信装置2と第2のAVコンテンツ受信装置3とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、AVコンテンツを解読するための暗号化鍵Kc oの種を要求するコマンドを送信してくるAVコンテンツ受信装置が、全て拡張暗号化手法を使用することができるAVコンテンツ受信装置である場合、暗号化手法を基本暗号化手法から拡張暗号化手法に切り替えるとしてもよい。

【0089】また、上述した実施の形態1では、AVコンテンツ送信装置1が暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるさい、まず、AVコンテンツ送信装置1は、第2のAVコンテンツ受信装置3との間で互いに認証を行い、その認証が成功すると、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるとした。しかしながら、図5に示すように、AVコンテンツ送信装置1は、第2のAVコンテンツ受信装置3からの認証要求を受信した後(図5のステップ1)、互いの認証が成功するか否かにかかわらず、暗号化手法を拡張暗号化手法から基本暗号化手法へ変更し(図5のステップ2)、その変更の後、認証が成功すると(図5のステップ3)、暗号化手法を基本暗号化手法に決定するとしてもよい(図5のステップ5)。なお、図5のステップ3で認証が失敗すると、暗号化手法を基本暗号化手法から拡張暗号化手法に再変更して暗号化手法を決定するとしてもよい(図5のステップ4)。

【0090】また、上述した実施の形態1では、AVコンテンツ送信装置1は、第2のAVコンテンツ受信装置3との間で互いに認証を行い、その認証が成功した場合に、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるとした。しかしながら、AVコンテンツ送信装置1は、第2のAVコンテンツ受信装置3からの認証要求を受信すると、認証が成功するか失敗するかにかかわらず、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えて、その切り替えた後の基本暗号化手法でAVコンテンツを暗号化して出力してもよい。ただしこの場合、AVコンテンツ送信装置1と第2のAVコンテンツ受信装置3との間での認証が失敗すると、AVコンテンツ送信装置1は、第2のAVコンテンツ受信装置3に交換鍵Kexを出力しない。したがって、AVコンテンツ送信装置1からのAVコンテンツは、不正な装置に解読されないように保護される。他方、AVコンテンツ送信装置1が第2のコンテンツ受信装置3からの認証要求を受信して、暗号化手法を基本暗号化手法に切り替えて暗号化したAVコンテンツを出力する場合、上述した実施の形態1で説明したとおり、第1のコンテンツ受信装置2は、AVコンテンツ送信装置1からの、暗号化手

法が基本暗号化手法に切り替わるという情報を入力し、AVコンテンツ送信装置1からの基本暗号化手法で暗号化されたAVコンテンツを入力して、基本暗号化手法でそのAVコンテンツを解読することになる。一方その後、AVコンテンツ送信装置1は、第2のコンテンツ受信装置3が不正であると判断した時点で、拡張暗号化手法に再変更する。

【0091】さらに、請求項10の本発明は、請求項1から9のいずれかに記載のAVコンテンツ送信方法の各ステップの全部または一部を実現するためのプログラムを格納したことを特徴とする媒体である。また、請求項13の本発明は、請求項11または12記載のAVコンテンツ受信方法の各ステップの全部または一部を実現するためのプログラムを格納したことを特徴とする媒体である。

【0092】

【発明の効果】以上説明したところから明らかなように、本発明は、AVコンテンツ送信装置が第1の暗号化手法で暗号化したAVコンテンツを送信しているときに、その第1の暗号化手法を使用することができないAVコンテンツ受信装置がそのAVコンテンツを解読することができるようにするAVコンテンツ送信方法を提供することができる。

【0093】また、本発明は、第1の暗号化手法で暗号化したAVコンテンツを送信しているときに、その第1の暗号化手法を使用することができないAVコンテンツ受信装置がそのAVコンテンツを解読することができるようにするAVコンテンツ送信装置を提供することができる。

【0094】また、本発明は、上述したAVコンテンツ送信方法を用いたさい、第1の暗号化手法で暗号化されたAVコンテンツを受信し解読していた、第1の暗号化手法を使用することができないAVコンテンツ受信装置とは別のAVコンテンツ受信装置がある場合、その別のAVコンテンツ受信装置が引き続きそのAVコンテンツを解読することができるようにするAVコンテンツ送信方法およびAVコンテンツ受信方法を提供することができる。

【0095】さらに、本発明は、上述したAVコンテンツ送信装置が第1の暗号化手法を使用することができないAVコンテンツ受信装置にそのAVコンテンツを解読させる場合、そのAVコンテンツ受信装置とは別に、第1の暗号化手法で暗号化されていたAVコンテンツを引き続き解読するAVコンテンツ受信装置を提供することができる。

*【図面の簡単な説明】

【図1】本発明の実施の形態1のAVコンテンツ通信システムのブロック図

【図2】本発明の実施の形態1のAVコンテンツ通信システムのAVコンテンツ送信装置1が送信するAVコンテンツおよびコマンドを含むデータの構成図

【図3】本発明の実施の形態1のAVコンテンツ通信システムのAVコンテンツ送信装置1の動作の一部を示すフローチャート

【図4】本発明の実施の形態1のAVコンテンツ通信システムの第1のAVコンテンツ受信装置2の動作の一部を示すフローチャート

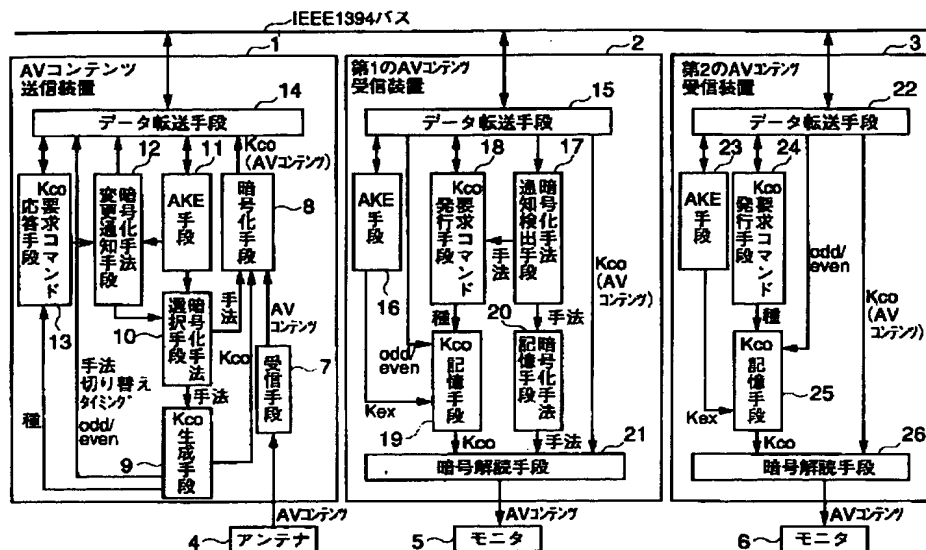
【図5】図3とは異なる、本発明の実施の形態1のAVコンテンツ通信システムのAVコンテンツ送信装置1の動作の一部を示すフローチャート

【図6】本発明の課題を説明するための図

【符号の説明】

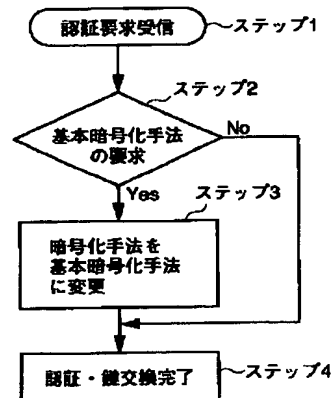
- 1 AVコンテンツ送信装置
- 2 第1のAVコンテンツ受信装置
- 3 第2のAVコンテンツ受信装置
- 4 アンテナ
- 5、6 モニタ
- 7 受信手段
- 8 暗号化手段
- 9 Kc o生成手段
- 10 暗号化手法選択手段
- 11 AKE手段
- 12 暗号化手法変更通知手段
- 13 Kc o要求コマンド応答手段
- 14 データ転送手段
- 15 データ転送手段
- 16 AKE手段
- 17 暗号化手法通知検出手段
- 18 Kc o要求コマンド発行手段
- 19 Kc o記憶手段
- 20 暗号化手法記憶手段
- 21 暗号解読手段
- 22 データ転送手段
- 23 AKE手段
- 24 Kc o要求コマンド発行手段
- 25 Kc o記憶手段
- 26 暗号解読手段
- 27 送信装置
- 28 パソコン
- 29 セットトップボックス（衛星放送受信機）

【図1】

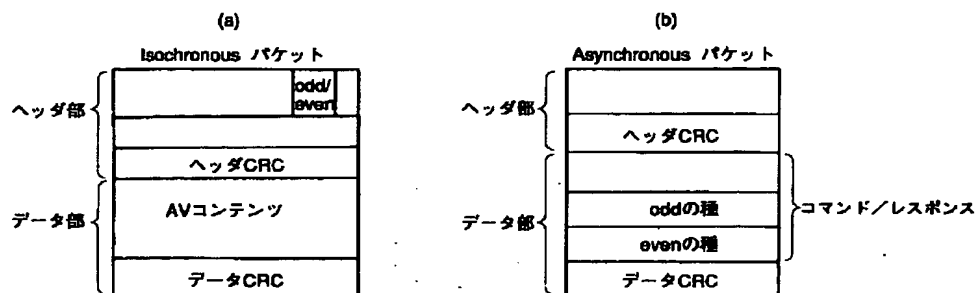


【図3】

AVコンテンツ送信装置1の動作

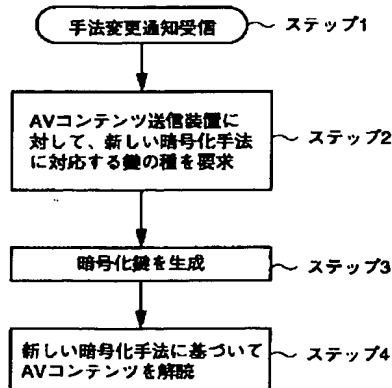


【図2】

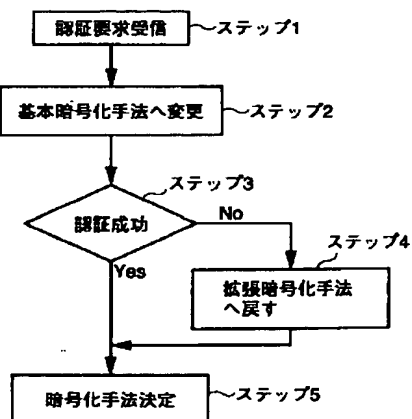


【図4】

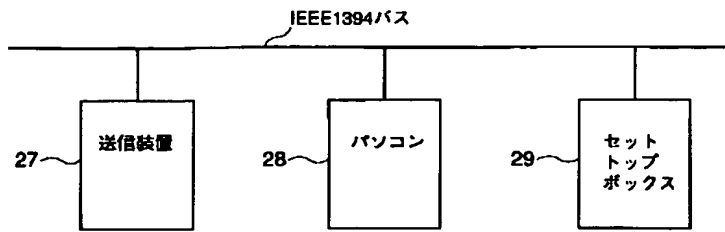
第1のAVコンテンツ受信装置2の動作



【図5】



【図 6】



フロントページの続き

(51) Int. Cl. ⁶

識別記号

F I

H O 4 L 29/08

H O 4 L 9/00

6 7 3 B

H O 4 N 7/167

13/00

3 0 7 Z

// G O 6 F 13/38

3 5 0

H O 4 N 7/167

Z

H O 4 L 12/28

H O 4 L 11/00

3 1 0 D

(72) 発明者 後藤 昌一

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 武知 秀明

大阪府門真市大字門真1006番地 松下電器
産業株式会社内